Cyber Security Governance, Risk & Compliance Masterclass

9 – 13 August 2027
Paris (France)



Cyber Security Governance, Risk & Compliance Masterclass

Ref: 322406_198175 **Date:** 9 – 13 August 2027 **Location:** Paris (France) **Fees:** 5900 GBP

Why This Course

Cybersecurity governance is no longer limited to technical controls; it is now closely connected to legal accountability, organizational risk management, regulatory compliance, and reliable records management. Modern organizations need structured governance frameworks that align information security practices with recognized standards, legal obligations, and effective documentation controls.

This intensive 1-week Cybersecurity Information Governance, Legal Risk Management, and ISO Records Management Controls Training program provides participants with a practical understanding of cybersecurity governance, ISO 27001-aligned information security management, legal risk assessment, and ISO 15489 records management controls. Through case studies, policy development exercises, mock audits, and incident response simulations, participants will learn how to integrate governance, risk, compliance, and records management into a stronger cybersecurity framework.

What You'll Learn and Practice

By joining this program, you will:

- Understand the principles of cybersecurity governance and organizational risk management.
- Explore key regulatory frameworks, standards, and compliance expectations.
- Establish governance structures that support cybersecurity accountability.
- Understand ISO 27001 requirements and their role in information security management.
- Implement and improve an Information Security Management System.
- Apply cybersecurity risk assessment and treatment approaches.
- Identify and assess legal risks related to cybersecurity.
- Manage compliance with data protection regulations and breach notification requirements.
- Address contractual risks and third-party security obligations.
- Apply ISO records management controls in cybersecurity contexts.
- Integrate records management with information security and compliance activities.
- Develop cybersecurity policies, procedures, audit practices, and incident response plans.



The Program Flow

Day 1: Foundations of Cybersecurity Governance

- Understand the principles and purpose of cybersecurity governance.
- Explore key regulatory frameworks, standards, and governance models.
- Identify the role of leadership in setting cybersecurity direction and accountability.
- Establish a cybersecurity governance framework aligned with organizational objectives.
- Connect governance practices with risk management, compliance, and operational resilience.

Day 2: Information Security Management Systems

- Understand ISO 27001 requirements and core ISMS concepts.
- Explore the steps for implementing an Information Security Management System.
- Apply risk assessment and risk treatment approaches within an ISMS.
- Understand internal controls, monitoring, and documentation requirements.
- Review continuous improvement and ISMS auditing practices.

Day 3: Legal Risk Management in Cybersecurity

- Identify legal risks associated with cybersecurity incidents and data protection failures.
- Assess compliance obligations under data protection regulations such as GDPR.
- Understand contractual risks and third-party security responsibilities.
- Explore legal considerations in incident response and breach notification.
- Develop mitigation strategies for reducing legal, regulatory, and reputational exposure.

Day 4: ISO Records Management Controls

- Understand ISO 15489 principles for records management.
- Apply records management controls within cybersecurity and compliance environments.
- Integrate records management with information security governance.
- Ensure effective documentation, retention, access, and evidence management.
- Use reliable record-keeping to support compliance, audits, and incident investigations.

Day 5: Practical Application and Case Studies

- Develop a comprehensive cybersecurity policy aligned with governance and compliance needs.
- Conduct a mock security audit to assess controls and documentation.
- Build and review incident response plans and escalation procedures.
- Participate in an incident response simulation.
- Complete a final case study integrating governance, legal risk, compliance, and records management.



Individual Impact

- Build confidence in applying cybersecurity governance principles.
- Strengthen understanding of ISO 27001, ISMS, and ISO records management controls.
- Improve legal risk assessment and compliance management capabilities.
- Develop practical skills in cybersecurity policy and procedure development.
- Gain experience in audits, incident response planning, and governance integration.

Work Impact

- Strengthen organizational cybersecurity governance and accountability.
- Improve alignment with ISO standards, legal requirements, and compliance expectations.
- Reduce legal, regulatory, and operational risks linked to cybersecurity incidents.
- Enhance audit readiness through better records management and documentation.
- Support stronger cybersecurity policies, procedures, and risk mitigation practices.

Training Methodology

This program combines governance concepts with practical implementation through:

- Cybersecurity governance case studies and framework discussions.
- ISO 27001 and ISMS implementation exercises.
- Legal risk assessment and compliance scenario analysis.
- ISO records management control mapping activities.
- Cybersecurity policy development workshops.
- Mock audits, incident response simulations, and final integrated case study.

Beyond the Course

Upon completion, participants will be able to:

- Design and implement a cybersecurity governance framework.
- Support ISMS implementation aligned with ISO 27001 principles.
- Conduct legal risk assessments in cybersecurity contexts.
- Align organizational practices with ISO information and records management standards.
- Develop and apply cybersecurity policies, procedures, and incident response plans.

